

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Information associated with the Google Account  
[REDACTED] and Gmail [REDACTED]@gmail.com  
that is stored at premises controlled by Google LLC

Case No. 2:24-mj-113

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 875(c)	Interstate Communications with Threat to Kidnap or Injure
18 U.S.C. § 922(g)(4)	Possession of a firearm by a prohibited person

The application is based on these facts:

See attached affidavit of FBI SA Brock Flint

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Brock Flint

Applicant's signature

Brock Flint, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: March 1, 2024

City and state: Columbus, OH

Kimberly A. Jojon  
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
GOOGLE ACCOUNT [REDACTED] AND  
GMAIL [REDACTED]@GMAIL.COM  
THAT IS STORED AT PREMISES  
CONTROLLED BY GOOGLE LLC

Case No. 2:24-mj-113

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Brock Flint, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Google LLC (“Google”), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and am assigned to the Columbus Resident Agency of the Cincinnati Field Office. I have been employed as a Special Agent since March 17, 2019, and have participated in numerous

investigations. I am presently assigned to the Joint Terrorism Task Force, based in Columbus, Ohio. Before my employment with the FBI, I was an Explosive Ordnance Disposal specialist with United States Air Force, specializing in Improvised Explosive Devices. I have an undergraduate degree in Security and Intelligence, focused on terrorism. I have worked numerous investigations focused on crimes committed using social media and other Internet mediums.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 875(c) (Interstate Communications with Threat to Kidnap or Injure) and 18 U.S.C. § 922(g)(4) (Possession of a Firearm by a Prohibited Person) (the “Target Offenses”) have been committed [REDACTED]. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

1. In late 2023, the FBI received information from a source relating to [REDACTED]. The source provided copies of text messages from [REDACTED]. The source has no criminal history.

The source received no compensation for the information; FBI investigators believe he<sup>1</sup> provided information out of concern regarding [REDACTED] conduct. More recently, the source, as he learned the extent of the FBI investigation into [REDACTED] has ceased to cooperate with investigators.

2. The FBI learned that [REDACTED] had been committed, pursuant to an order by the Licking County Court of Common Pleas, in case number [REDACTED], in November 2014 to Twin Valley Behavioral Healthcare Hospital, after the Licking County Court found “probable cause to believe that [REDACTED] [was] a mentally ill person subject to court order.” The FBI has sought records from the Licking County Court of Common Pleas pertaining to [REDACTED] including records in case number [REDACTED]. In response to a subpoena, the Licking County Court of Common Pleas indicated they had no records pertaining to [REDACTED] and also indicated that case number [REDACTED] had been expunged.

3. FBI investigators are looking for records elsewhere as to whether [REDACTED] “has been adjudicated as a mental defective or who has been committed to a mental institution.” The Office of the Ohio Attorney General indicated to investigators that it had no records pertaining to [REDACTED] in their mental incompetency database and in their criminal history database.

4. On or about October 1, 2021, a Licking County municipal court probation officer visited [REDACTED] home, while supervising [REDACTED] as a result of an OVI (operating a vehicle impaired) conviction. During the visit, the officer located an AR-15 style firearm. The firearm was not confiscated, due to the officer’s belief at that time that [REDACTED] was not prohibited from

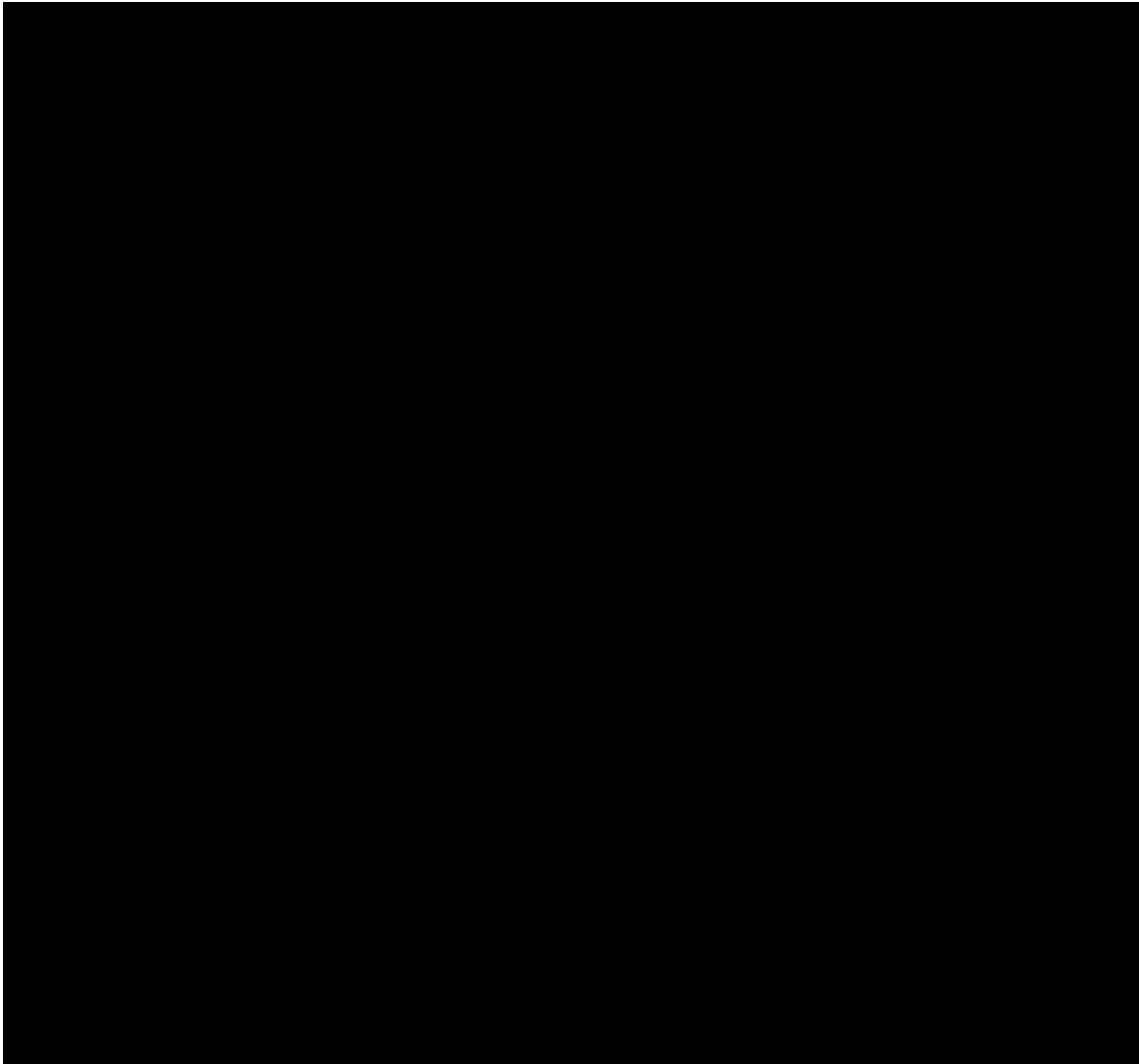
---

<sup>1</sup> For purposes of this affidavit, masculine pronouns will be used to refer to the source. I make no representation as to whether the source is a male or female.

possessing the firearm. According to the source, [REDACTED] had purchased the firearm a few years ago.

5. Based on my training and experience, I know that individuals may use their cellular phones to research firearms and to take pictures of the firearms they possess.

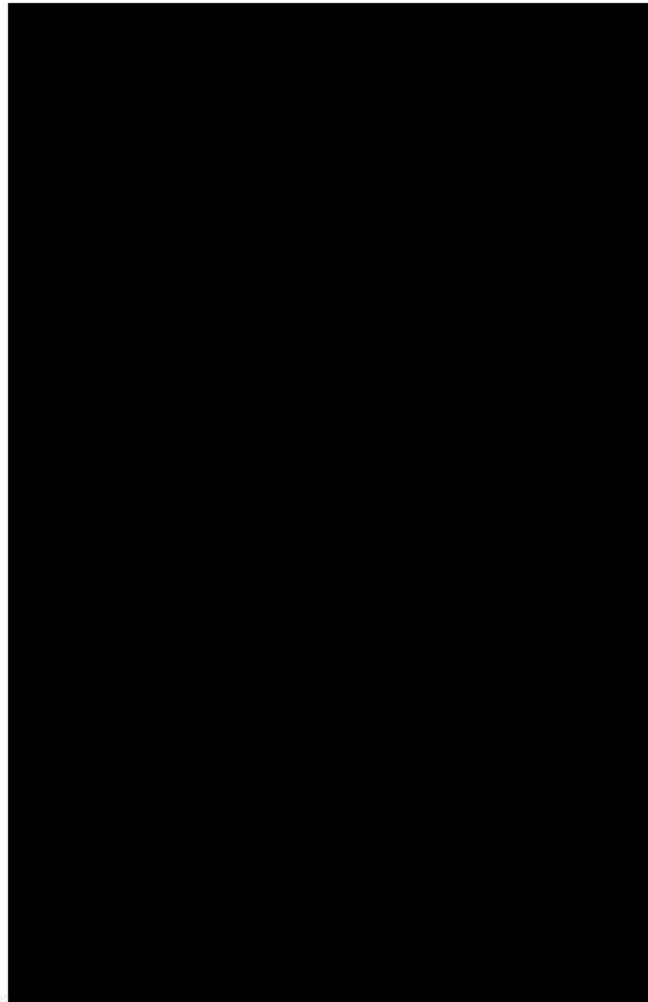
6. The aforementioned source also provided FBI investigators with approximately 100 screenshots of text messages from [REDACTED] to the source, wherein [REDACTED] reveals a hatred for individuals who are Jewish. A series of text messages on or about November 6, 2023, from [REDACTED] to the source are provided below.





7. As referenced in the above, [REDACTED] used derogatory terms to refer to Jewish people, including “Jew parasite” and “kike,” which I know from my training, experience, and research to be commonly known slurs. [REDACTED] further stated, “If u EXTERMINATE all of it,” referring to Jews, then “it won’t come back.” [REDACTED] also made reference to a future “hunt,” stating, “[W]hen the hunt starts, your anchor women on most news stations are going to go too. They are either are [sic] Jews, are married to Jews, or have done sexual favors for Jews, all of which are treason and punishable by death.”

8. In another string of text messages, below, with the source, [REDACTED] shared a link to a YouTube video.



9. The link above leads to a video on YouTube posted by “Long Island Audit” that appears to depict an incident at a police station. After sharing the link, [REDACTED] commented again about “hunting,” stating, “I’m talking about hunting Jews so, don’t comment, it’s a message. Most Jews I deleted on my page anyway, just a couple left in including fake friends like [REDACTED] and my message is designed to intimidate his Jew ass. Subliminal message. [Two emojis.]” As he has done in other messages, [REDACTED] referenced a future event, stating, “They will be hunted pretty soon.”

10. The source communicated to investigators that he understood [REDACTED] in the aforementioned text messages referencing “friends,” deleting people from his “page,” and



“subliminal message,” to be referring to [REDACTED] Facebook page and [REDACTED] Facebook friends. The source only knew of [REDACTED] Facebook account and did not believe [REDACTED] had other social media accounts.

11. In another pair of texts on October 11, 2023, below, [REDACTED] indicated that he had “deleted all of the Jews off my Facebook page today except for Little [REDACTED].” [REDACTED] also made reference to a future event, stating “Yeah u definitely don’t want to be thought of as a Jew sympathizer for what is coming up,” and “Lots of fun to be had soon by a lot of people. I’m definitely going to be an interrogation specialist.”





12. Attempts by agents to view [REDACTED] Facebook page have been unproductive since his page is set to private. As a result of the evidence gathered thus far in the investigation, including the aforementioned text messages and [REDACTED] statements in those messages, I believe [REDACTED] was posting on his Facebook page with the intent to intimidate or threaten Jewish individuals, and he may have used or may be using Facebook Messenger to intimidate or threaten them.

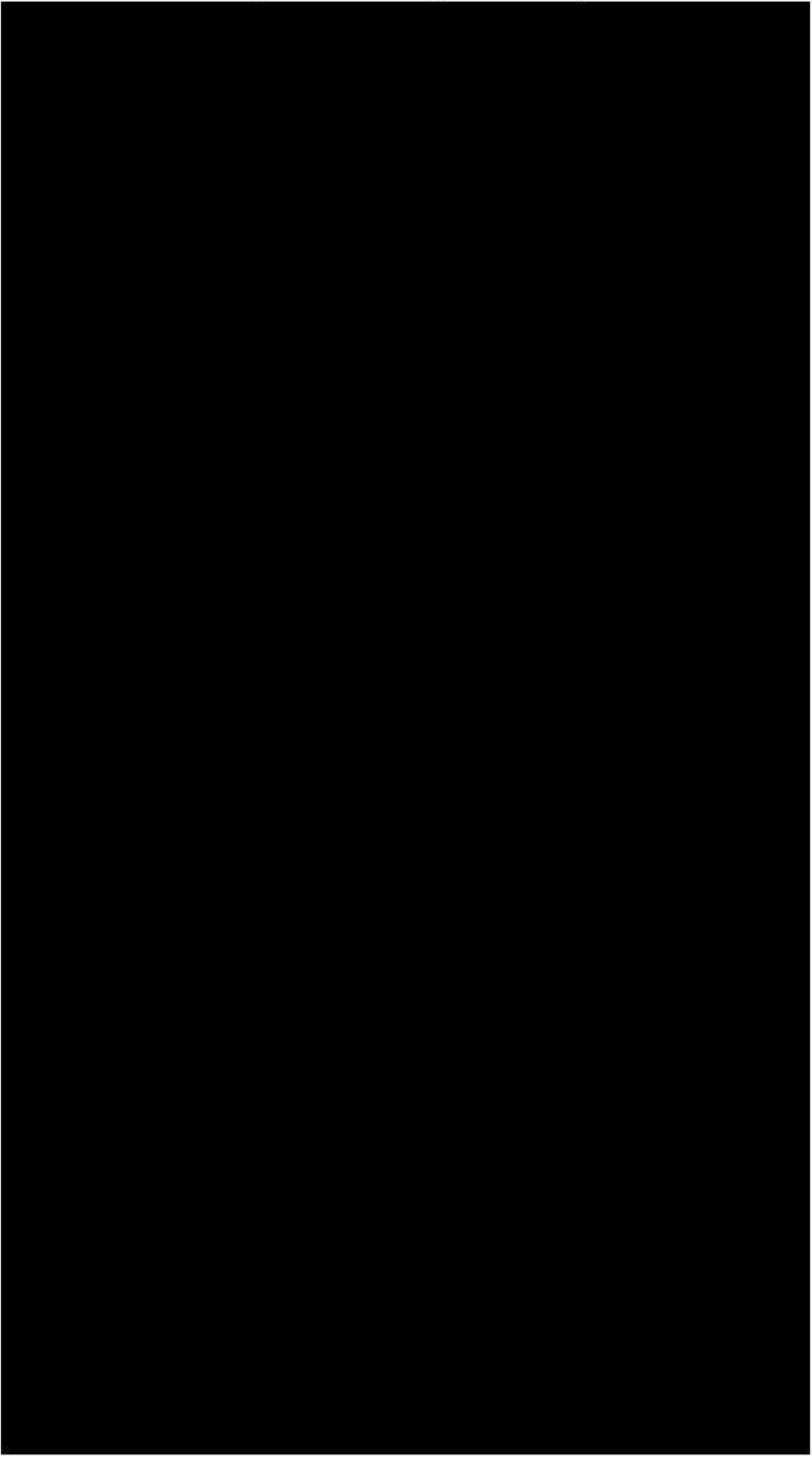
13. Investigators have utilized legal process to verify that Facebook account [REDACTED] is used by subscriber [REDACTED], utilizing the vanity name [REDACTED]. I know [REDACTED] middle name to be [REDACTED]

14. Furthermore, investigators obtained a court order authorizing the implementation of a Pen Register and Trap and Trace device ("PRTT") on a Verizon Wireless cellular telephone number subscribed to by [REDACTED]. After the PRTT was implemented, investigators observed that the data from the PRTT, over the course of approximately one week, included hundreds of messages that were designated as "Not Available." Based on my training and experience and my knowledge of data from PRTT devices, I believe that these "Not Available" messages are indicative of [REDACTED] using an encrypted or third-party messaging platform, such as Facebook Messenger, WhatsApp or Signal, on his cellular phone.

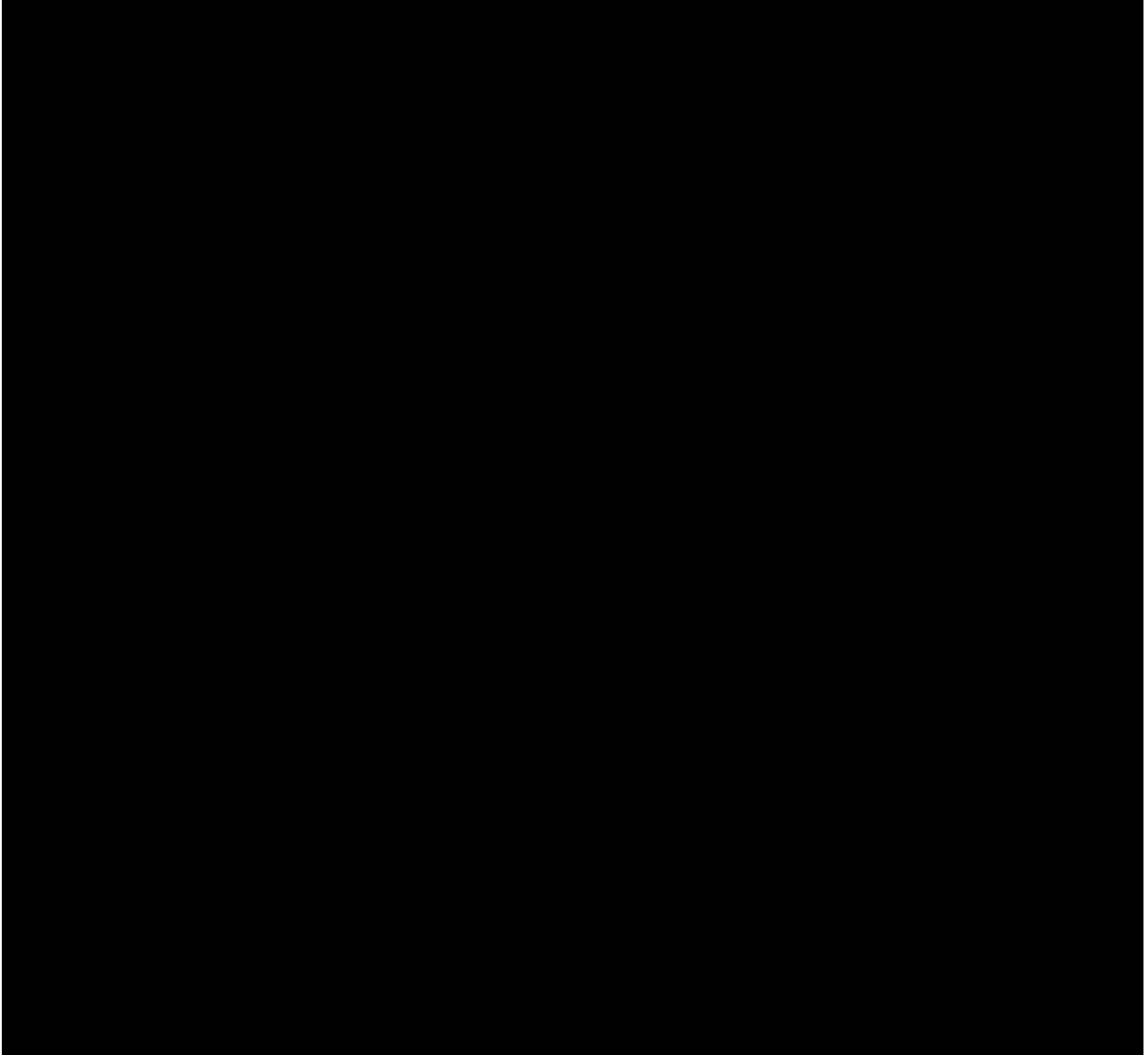
15. Based on my review of the text messages from [REDACTED] that the source provided, [REDACTED] espouses a racially motivated violent extremist ("RMVE") ideology. This is reflected in [REDACTED] sharing of memes lauding Hitler, and [REDACTED] antisemitic rhetoric. [REDACTED] shared the below meme and screenshot with the source, stating Hitler's spirit will be returning. Similar to [REDACTED] language in some of his text messages and the language in some of the images/memes that [REDACTED] has shared with the source, [REDACTED] referenced a future event stating, "His Spirit is rising

again and when it has fully arisen, ...” [REDACTED] also asked the recipient of his message whether the recipient would “follow [Hitler] this time.” Investigators assess that, in light of the investigation,

including [REDACTED] veneration of Hitler and his violent language about hunting Jews, that [REDACTED] may be preparing to commit violence against a minority community.



In another text message that [REDACTED] sent to the source, [REDACTED] shared a violent and gory image from a 4chan message board, showing his desensitization towards violence. The message's caption stated, "I am a terrorist. I am a racist. I am an antisemite. I am death and I am coming for you." Similar to [REDACTED] text messages, the caption on this image included a reference to a future event with the statement, "I am coming for you."



16. In other text messages, [REDACTED] has sent a link to a 4chan.org website (the link reads, "IDF is making us choose sides.") and to images posted on Gab.com (the image reads,

“The Zionist position is that Jews must have Nationalism but Whites cant because this would exclude Jews from the positions of power in White countries they use to further Jewish interests.”). Based on my training and experience, I know that 4chan.org and Gab.com are websites where users frequently espouse RMVE language.

17. In multiple other messages, [REDACTED] has referenced a “hunt” and/or a future event. Shortly after midnight on August 19, 2023, [REDACTED] sent a message to the source which read, “I’m going to keep posting about hunting season and, please stop commenting [emoji]. There is a method to my madness.” Later in the day, [REDACTED] sent a message to the source, reading, “Scary lol. U have no idea what’s coming.” The source responded, “Sure I do just don’t care.” [REDACTED] then responded, “That’s u. Lots of people DO care tho[.] And are awaiting to have fun lots if it lol.” In another series of messages, [REDACTED] commented about court cases, and then stated, “It’s coming lol[.] I’m not going to have to pay for my first house, one of the traitors who forfeits theirs will become mine lol.” Later in the same string of messages, [REDACTED] stated, “Yeah um, u have no idea what is coming [laughing emoji].” In another conversation with the source, after the source asked why [REDACTED] was turning on him, [REDACTED] responded, “Soon u will see and be embarrassed and u can join the other Jew lovers there is group of of you don’t worry.” Later in the same conversation, [REDACTED] stated, “I’ll take you back, but not [REDACTED] and honestly, payback is going not be fun when this collapses soon [thumbs up emoji].” [REDACTED] then shared images, including antisemitic images, with the source. In response to the source asking, “What is supposed to be collapsing,” [REDACTED] shared images antisemitic images from 4chan. [REDACTED] later stated, “But seriously, when this collapses, hunters are going to pretty much have free reign to hunt whoever just like Soviet collapse, only except, this one is going to be much worse than

Soviet collapse because of different circumstances FYI,” and “The Jew problem is more pronounced here and all the Jews who aren’t in Israel are HERE!!”

18. According to legal process, [REDACTED] utilizes a Motorola XT2215DL smartphone, utilizing an Android operating system. Android is an operating system owned and operated by Google. Through my experience, I know that Android operating systems usually back up to (i.e. save data from a user’s cellular phone to) the user’s Google account. Based on my training and experience, I believe that [REDACTED] is utilizing a Google account to back up the data on his cellular phone, to include any saved screenshots or fruits of his criminal behavior. I submit that there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of the Target Offenses is stored in [REDACTED] Google account.

#### **BACKGROUND CONCERNING GOOGLE**<sup>2</sup>

19. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service

---

<sup>2</sup> The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the “Google legal policy and products” page available to registered law enforcement at [lens.google.com](https://lens.google.com); product pages on [support.google.com](https://support.google.com); or product pages on [about.google.com](https://about.google.com).

called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

20. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

21. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

22. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

23. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

24. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as



contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them.

25. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.

26. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

27. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

28. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

29. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.)

and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

30. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after

eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

31. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

32. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users.

According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

33. Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

34. Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

35. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are

displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

36. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

37. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

38. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a

communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

39. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. The data sought by the FBI will indicate whether [REDACTED] has made any affirmative actions towards initiating his "hunt," such as researching or visiting synagogues or other locations frequented by Jewish people, including Jewish individuals' residences, and will also provide evidence of the Target Offenses. The information sought will enable Agents to determine whether [REDACTED] is unlawfully threatening any individuals, especially if he is doing so due to his perception that they are Jewish.

40. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. The text messages provided by the source, with screenshots, were first saved on [REDACTED] phone. Since they were saved to his phone, they would be saved to his Google account, and accessible via this search warrant to Google LLC.

41. Agents have utilized legal process to establish that [REDACTED] utilizes a Motorola phone with an Android operating system, and he is the owner of the Google account [REDACTED] via phone number [REDACTED] and Gmail account [REDACTED]



██████████@gmail.com. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

42. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

43. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. Given my training and experience and my knowledge of this investigation, I believe that ██████████ may possibly be using apps, such as Facebook Messenger, Gab, Truth Social, some of which provide greater anonymity, to engage in his conduct. In

addition, emails, instant messages, Internet activity, documents, and contact can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

44. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

### CONCLUSION

45. Based on the forgoing, I request that the Court issue the proposed search warrant.

46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Brock Flint

---

Brock Flint  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on March 1, 2024

  
Kimberly A. Johnson  
United States Magistrate Judge



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with Google account [REDACTED] and [REDACTED]@gmail.com (“the Account”) that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google LLC (“Google”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google. Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from 1 June 2023 to the date of the signing of this warrant, unless otherwise indicated:

- a. All business records and subscriber information, in any form kept, pertaining to the Account, including:
  1. Names (including subscriber names, user names, and screen names);
  2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
  3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
  4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions, including log-in IP addresses;
  5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
  6. Length of service (including start date and creation IP) and types of service utilized;
  7. Means and source of payment (including any credit card or bank account number); and
  8. Change history.

- b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs
- d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails. All forwarding or fetching accounts relating to the accounts;
- e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
- f. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;
- g. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.
- h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third party application associated with each

record; and all associated logs, including access logs and IP addresses, of each record.

- i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.
- j. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers;
- k. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.
- l. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.
- m. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 875(c) (Interstate Communications with Threat to Kidnap or Injure) and 18 U.S.C. § 922(g)(4) (Possession of a firearm by a prohibited person) (the “Target Offenses”), those violations involving [REDACTED], including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

- a. On or after June 1, 2023, any steps, including preparatory steps, taken in furtherance of [REDACTED] scheme to commit any act of violence against a person because of their religious or cultural identity, including because the person practices the Jewish religion, identifies as Jewish, or is perceived as Jewish.
- b. On or after June 1, 2023, whether [REDACTED] is working with any other individuals to effectuate any violence against a person because of their religious or cultural identity, including because the person practices the Jewish religion, identifies as Jewish, or is seen as being Jewish.
- c. On or after June 1, 2023, whether [REDACTED] has used websites, text messages, or other social media applications to engage in harassment or intimidation of another person, particularly if motivated by the person’s religious or cultural identity.
- d. On or after June 1, 2023, whether [REDACTED] has made any statements threatening violence toward any individual;
- e. On or after June 1, 2023, whether [REDACTED] has stalked any individual, which would be reasonably expected to cause substantial emotion distress to the person, their immediate family member, their spouse or their intimate partner;
- f. Whether [REDACTED] has possessed any firearms or ammunition;
- g. Whether [REDACTED] has been adjudicated as a mental defective;
- h. Whether [REDACTED] has been committed to any mental institution;
- i. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the Target Offenses and to the email account owner;
- j. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).



- k. The identity of the person(s) who communicated with the Account about matters relating to the Target Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [[**CHOOSE APPLICABLE:** Google LLC **AND/OR** Google Payment Corporation]] (“Google”), and my title is \_\_\_\_\_.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google’s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature